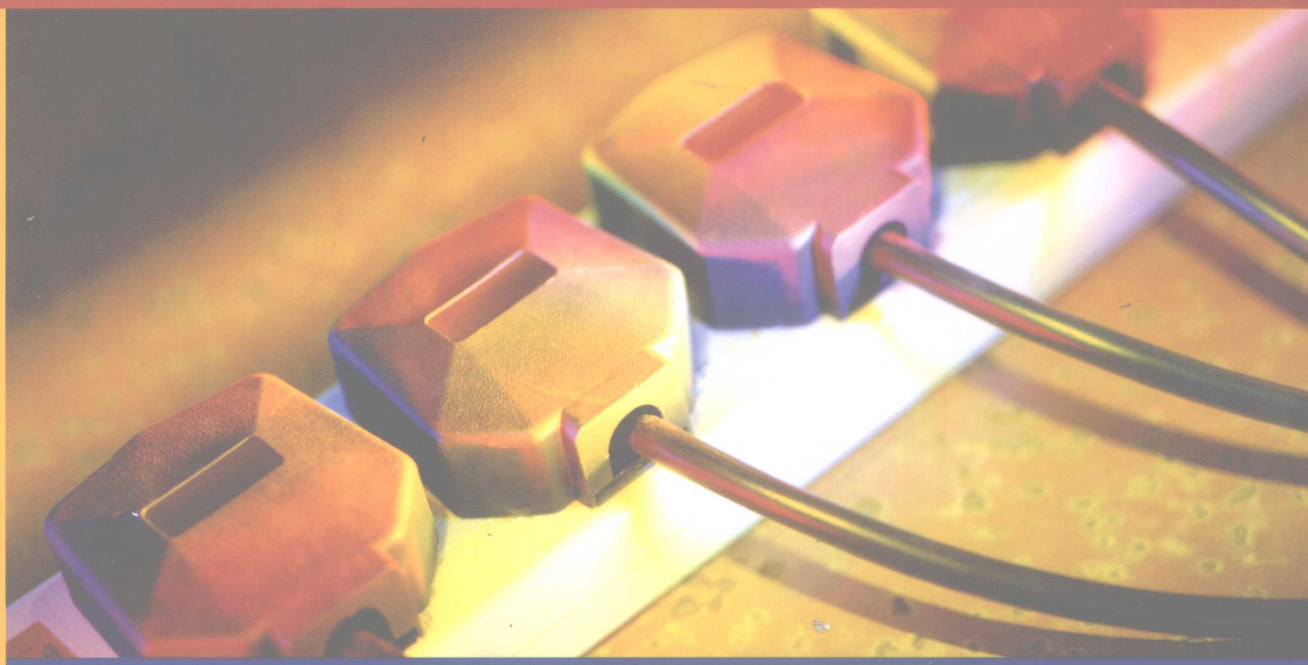
普通高等教育“十一五”国家级规划教材

高等院校信息与通信工程系列教材

网络安全协议理论与技术



范明钰 王光卫 编著

清华大学出版社

ISBN 978-7-302-19300-5

定价：24.00元

普通高等教育“十一五”国家级规划教材

高等院校信息与通信工程系列教材

网络安全协议理论与技术

范明钰 王光卫 编著

清华大学出版社
北京

内 容 简 介

本书从基本概念入手，通过 Internet 协议的实际例子，建立网络协议的概念，分析了 Internet 协议不安全的原因，介绍了安全协议的密码学基础，分析了安全协议与密码学的关系，介绍了利用不同的密码算法建立安全信道。从第 4 章开始，介绍基本的安全协议、抗攻击的安全协议和实际使用的安全协议。附录中介绍了最新的几类密码算法。每章都附有重点和难点分析，并附有习题与思考题。

全书共分为三个部分：第一部分介绍基本概念和 Internet 中的协议（第 1 章和第 2 章）。第二部分介绍安全协议，分为三个内容、安全协议的密码学基础（第 3 章）、基本安全协议（第 4 章）和抗攻击的安全协议（第 5 章）。第三部分介绍实际使用的安全协议（第 6 章）。这三个部分基本上是关联的，既可以从概念入手讲解，也可以先从实际例子开始最后得到理性的知识。

本书可供工科类计算机、电子信息、通信等相关学科的本科学生和研究生使用。

图书在版编目(CIP)数据

网络安全协议理论与技术/范明钰，王光卫编著. 北京：清华大学出版社，2009.2
（高等院校信息与通信工程系列教材）
ISBN 978-7-302-19300-5

Ⅰ. 网… Ⅱ. ①范… ②王… Ⅲ. 计算机网络－安全技术－通信协议－高等学校－教材
Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2009)第 006103 号

责任编辑：陈国新
责任校对：白　蕾
责任印制：李红英
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京市昌平环球印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：15　**字　数**：347 千字
版　　次：2009 年 2 月第 1 版　　**印　　次**：2009 年 2 月第1 次印刷
印　　数：1～3000
定　　价：24.00 元

出版说明

信息与通信工程学科是信息科学与技术的重要组成部分。改革开放以来，我国在发展通信系统与信息系统方面取得了长足的进步，形成了巨大的产业与市场，如我国的电话网络规模已位居世界首位，同时该领域的一些分支学科出现了为国际认可的技术创新，得到了迅猛的发展。为满足国家对高层次人才的迫切需求，当前国内大量高等学校设有信息与通信工程学科的院系或专业，培养大量的本科生与研究生。为适应学科知识不断更新的发展态势，他们迫切需要内容新颖又符合教改要求的教材和教学参考书。此外，大量的科研人员与工程技术人员也迫切需要学习、了解、掌握信息与通信工程学科领域的基础理论与较为系统的前沿专业知识。为了满足这些读者对高质量图书的渴求，清华大学出版社组织国内信息与通信工程国家级重点学科的教学与科研骨干以及本领域的一些知名学者、学术带头人编写了这套高等院校信息与通信工程系列教材。

该套教材以本科电子信息工程、通信工程专业的专业必修课程教材为主，同时包含一些反映学科发展前沿的本科选修课程教材和研究生教学用书。为了保证教材的出版质量，清华大学出版社不仅约请国内一流专家参与了丛书的选题规划，而且每本书在出版前都组织全国重点高校的骨干教师对作者的编写大纲和书稿进行了认真审核。

祝愿《高等院校信息与通信工程系列教材》为我国培养与造就信息与通信工程领域的高素质科技人才，推动信息科学的发展与进步做出贡献。

北京邮电大学

陈俊亮

2004 年 9 月

前　言

本书的编写经历了近四年，主要作为信息安全类本科生和研究生的教学参考书。

全书从基本概念入手，通过 Internet 协议的实际例子，建立网络协议的概念，分析了 Internet 协议不安全的原因，介绍了安全协议的密码学基础，分析了安全协议与密码学的关系，介绍了利用不同的密码算法建立安全信道。从第 4 章开始，介绍基本的安全协议、抗攻击的安全协议和实际使用的安全协议。附录中介绍了最新的几类密码算法。每章都附有重点和难点分析，并附有习题与思考题。

本书共分为三个部分。

第一部分：基本概念和 Internet 中的协议（第 1 章和第 2 章）。

第二部分：安全协议，分为三个内容：安全协议的密码学基础（第 3 章）、基本安全协议（第 4 章）、抗攻击的安全协议（第 5 章）。

第三部分：实际使用的安全协议（第 6 章）。

本书的三个部分基本上是关联的，既可以从概念入手讲解，也可以先从实际例子开始最后得到理性的知识。

参与本教材编写的主要人员有：王庆先博士、朱大勇博士；实验室学生沈丹、丁旭阳、张涛，其中第 4 章和第 5 章的绝大部分插图以及附录是沈丹同学编制的。谨在这里向他们表示诚挚的谢意。

编　者

2008 年 10 月

目　录

第 1 章　基本概念

本章是网络安全协议中关于网络、安全及密码学的基础知识。

本章分 5 个小节，第 1.1 节介绍网络基础以及网络协议的概念；第 1.2 节介绍网络安全的概念；第 1.3 节介绍网络的协议；第 1.4 节介绍网络协议面临的威胁；第 1.5 节是本章重点和难点分析。

1.1　网络基础及网络协议的概念

简单地说，网络是由两台以上计算机借助于协议连在一起组成的“计算机群”，再加上相应“通信设备”组成的综合系统。

早期的计算机应用模式是单机，其发展过程有小型机、中型机、大型机。单台计算机能干很多事情。虽然计算机的速度越来越快、性能越来越高、容量越来越大，但还是存在一些美中不足。比如办公室为每个人都配备了一台最新式计算机，但是打印机的配备却成了问题。如果只为一台或者几台计算机配备打印机，那些没有配备打印机的人打印时就需要把文件用磁盘复制到有打印机的计算机上去打印，不仅麻烦，而且也耽误别人的时间。另一方面，如果给所有计算机都配备打印机，它们多数情况下是处于闲置状态，很明显这是一种浪费。如果只给一台或几台计算机配备打印机，而其他所有计算机都可以利用这些打印机，并且相互之间不影响工作，这就是资源共享。

可以在网络上共享的资源除了打印机之外，还有硬盘、光盘、绘图仪、扫描仪以及各类软件、文本和各种信息资源等。在网络中共享资源既节省了大量的投资和开支，又便于集中管理。

利用网络可以进行信息交换和信息的集中与分散处理，比如说一家公司，有生产部、仓储部、市场部、财务部等很多部门和分公司。这些部门和分公司在地理位置上并不在一起。但是作为一个现代化的大公司，各个业务部门需要随时知道其他部门的各种数据：分散的销售数据需要及时集中起来配合仓储部的库存和生产部的生产，分散的财务数据也需要随时送到财务部集中处理以配合公司的整体行动。诸如此类，称为信息交换和信息的集中与分散处理。这些都需要依托网络才能做到。

计算机网络并不是随着计算机的出现而出现的，而是随着社会对资源共享和信息交换与及时传递的迫切需要而发展起来的。它是现代计算机技术和通信技术密切结合的产物。说得准确一些，计算机网络就是利用通信设备和通信线路，把位于不同地点的计算机等设备相互联起来，用相应的协议软件实现资源共享和信息交换的系统。

早期的网络是一个单位的几台计算机用一根电缆串在一起，实现局部资源共享和信

息交换。今天的网络，把世界上百个国家的大大小小几千万台计算机连为一体，形成硕大无比像蜘蛛网一样的“怪物”，在全世界范围内实现全方位的资源共享和信息交换。这就是 Internet，也称为国际互联网或因特网。对于一个单位来说，只要把这个单位网络的对外连线往 Internet 一搭，网络性质就从根本上改变了，其外延与内涵都产生了根本的变化。

网络带来的好处主要体现在资源共享、信息交换与及时传递两个方面。就拿资源共享来说吧，一个办公室或者几个办公室只安装一台打印机而不耽误工作；一个公司或者图书馆只购买一份昂贵的软件，公司里所有人都可以随意使用；火车站或者航空公司售票处，把票务信息汇总后放在网上，任何人都可以随时在网上查阅，知道某一次列车或者航班还有多少张票。诸如此类，既节约资金，又减少重复劳动。

在网络中进行信息交换与及时传递好处则更大。因为有了计算机网络，《人民日报》就能在北京制完版后几分钟内，将版样传送到全国各地，甚至国外的印制点。这样，在早晨 6 点多钟便可以从报上知道报纸印制前半小时发生的新闻；也是因为有了网络，花都的农民在家中便可以把鲜花推销到世界各国；韶关的孩子坐在家中就可以上广州师范附中的网校，接受全国特级教师的课外辅导。可以这么说，正是因为可以通过网络进行远距离的信息交换和及时传递，网络改变了时空，人与人之间的距离变近了，地球变小了，信息变多了。

1.1.1 网络的构成和分类

计算机网络是计算机技术和数据通信技术紧密结合的产物。所谓计算机网络，通俗地讲，就是将地理位置不同的多个计算机系统通过通信设备和线路连接起来，以功能完善的网络软件（在协议控制下）实现网络中资源共享和数据交换的系统，见图 1-1。

图 1-1 网络的构成

一个用计算机联网的通信系统一般由 6 个部分组成。

(1) 信息(message)：包括文字、声音、图像等数据。

(2) 发送设备：又称“主机”(host)——各种信息处理设备(计算机等)。

(3) 接收设备：同发送设备。

(4) 通信设备：负责主机间的通信控制和通信处理。

(5) 传输媒介：各种电缆、光纤、无线电波等。

(6) 通信协议：通信规则(无协议的两台设备可以连接但无法通信，如同讲不同语言的两人无法对讲)。

网络可分为资源子网和通信子网两部分，见图 1-2。

其中，资源子网包括硬件资源(主机、终端、I/O 设备等)、软件资源、数据资源等，负责全网数据处理业务，向网络用户提供各种网络资源和网络服务；通信子网包括传输介质

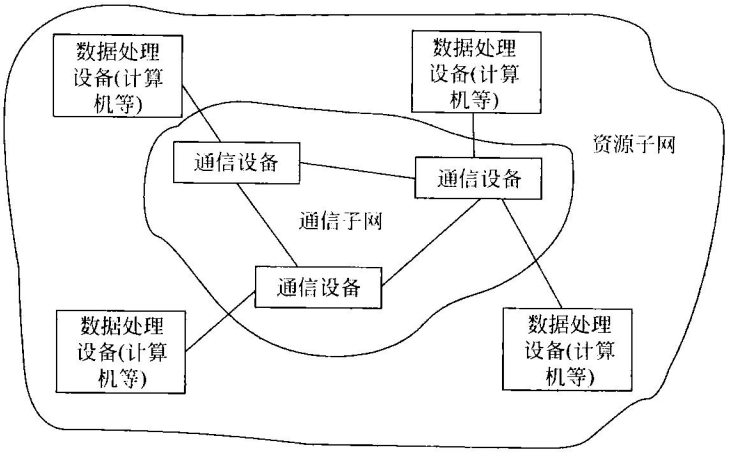


图 1-2　资源子网和通信子网

(电缆、光纤、无线电波等)、通信设备(交换机等),承担全网的数据传输、转接、加工和变换等通信处理工作。

按网络的规模和地理位置,网络可分为如下几种。

(1) 局域网(local area network,LAN):一般在小于 10km 的范围区域内,通常采用有线的方式连接起来。局域网通常用于一个单位、一座大楼或相应楼群之间,也特别适合于一个地域跨度不大的企业建立内部网,即 Intranet。

(2) 园区网:介于局域网和广域网之间的网络。

(3) 城域网(metropolitan area network,MAN):规模局限在一座城市的范围内,10～100km 的区域。

(4) 广域网(wide area network,WAN):网络跨越国界、洲界,甚至全球范围。Internet 是著名的广域网。

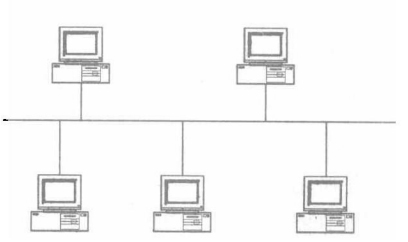


图 1-3　总线型网络拓扑

按网络权限关系,网络可分为内部网(intranet)和外部网(extranet)。

按照拓扑结构,网络可以分为总线型、星形、环形和网格网(全连网格网与不全连网格网),参见图 1-3 和图 1-4。

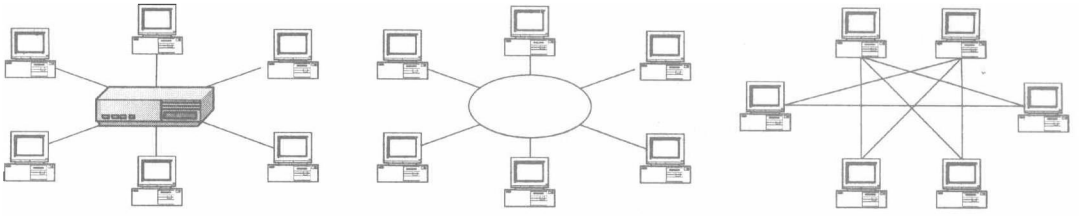


图 1-4　星形网络拓扑、环形以太网拓扑和网格网拓扑

按传输介质，网络可以分为如下几种。

（1）有线网：采用同轴电缆或双绞线来连接的计算机网络。因速度有限，技术落后，已被淘汰。

双绞线网是目前最常见的联网方式。它价格便宜，安装方便。因距离短，适于局域网内。

（2）光纤网：光纤网也是有线网的一种，但由于其特殊性而单独列出。光纤网采用光导纤维做传输介质，光纤传输距离长，传输率高，可达数千兆比特每秒，甚至更高，抗干扰能力强，不会受到电子监听设备的监听，是高安全性网络的理想选择。已被广泛应用。

（3）无线网：采用空间做传输介质，用电磁波作为载体来传输数据。由于联网方式灵活方便，是一种很有前途的联网方式。

1.1.2 网络的发展

计算机网络产生于20世纪60年代，如前所述，其发展动力主要有资源共享的需求、大型项目的合作，以及人与人之间的沟通需要。

按体系结构的发展来分，网络的发展过程大致可以分为以主机为中心的联机终端系统、以通信子网为中心的主机互联，以及具有层次化体系结构的标准化网络三个阶段。

1. 以主机为中心的联机终端系统

这种联机系统是早期网络的雏形，其特征主要是共享主机软硬件资源，其构成可分为单台主机（担负计算和通信任务）和多台终端（担负与用户的交互任务）。这种网络中，连接方式主要是本地或远程连接，如图1-5所示。

这种网络的例子有飞机订票系统，其中HOST为航空公司，终端为各订票点，采用的通信线路一般为电话线路。这种网络的缺点主要是主机负荷重，既要完成数据处理还要进行通信，此外线路利用率也低。对这种网络的改进方法是，终端集中器（集线器）加上主机的前端处理机，使通信任务与处理任务分离。

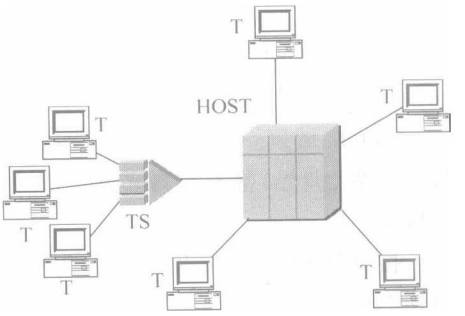


图1-5 以主机为中心的联机终端系统

2. 以通信子网为中心的主机互联

这种网络的特征是多个终端联机系统的互联，形成以多主机为中心的网络，网络结构从“主机-终端”转变为“主机-主机”，如图1-6所示。

3. 具有层次化体系结构的标准化网络的演变

主机-主机网络的演变如下。

（1）演变阶段1：通信任务从主机中分离，由通信控制处理机CCP完成，CCP是处理主机之间通信任务的专用计算机，见图1-7。